Date of Publication
December 12, 2022

Hive Pro

Hiveforce Labs

THREAT DIGEST

WEEKLY

Actors, Attacks, and Vulnerabilities

5 to 11 DECEMBER 2022

Summary

Threat Actors

Hive Pro discovered six Actors that have been active in the last week. Two of them (Lazarus Group, and Scattered Spider) are popular for financial crime. Three of them (BackdoorDiplomacy, Calisto, and APT37) are popular for Information theft and Espionage. Lastly, Agrius is an Iranian threat actor group popular for Sabotage and destruction. For further details, see the key takeaway section for Actors.

Attacks

We also discovered five new malware strains that have been active over the last week. Ransomware attacks are being launched against exposed Remote Desktop services (CVE-2019-0708) by five ransomware families that include BlackHunt, NYX, Redeemer, Vohuk, and Amelia are attacking open RDP ports. AppleJeus malware is used by the Lazarus group to steal the victim's private keys and exhausts crypto assets. The telecom industry is targeted by BackdoorDiplomacy with Irafau and Quarian backdoors. New ransomware called BlackMagic targets victims by using double extortion. The new botnet named Zerobot has two variants written in Go and is known to exploit known vulnerabilities. Bluelight, Dolphin, and Rokrat are used by group APT 37 and Fantasy Wiper is used by Agrius APT group. For further details, see the key takeaway section for Attacks.

Vulnerabilities

We discovered 32 Vulnerabilities last week that organizations should Prioritize. Among these 32, there were five zero-day, and three are undergoing reanalysis on NVD. For further details, see the key takeaway section for Vulnerabilities.

*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Key Takeaways

Threat Actors

Lazarus Group (AppleJeus)
The Lazarus threat actor employs fake cryptocurrency Apps with AppleJeus malware by masquerading Microsoft Office documents rather than the MSI installer. It was noticed that an unknown threat actor, DEV-0139 plotted attacks against the crypto industry.

Scattered Spider (unattributed)
The Scattered Spider leveraged CVE-2021-35464 to gain access to mobile carriers' networks from a Telco or BPO environment and performed SIM swapping.

BackdoorDiplomacy (Irafau, Quarian)
The BackdoorDiplomacy is an APT group aimed at a Middle Eastern telecom operator, successfully exploiting the ProxyShell flaw (CVE-2021-26855) to implant Irafau and Quarian backdoors.

Calisto (unattributed)
The Calisto is linked to spoofing Microsoft login pages of Global Ordnance, a legitimate U.S. military weapons and hardware supplier. A malicious PDF was sent to NGO officials using a spoofed email address.

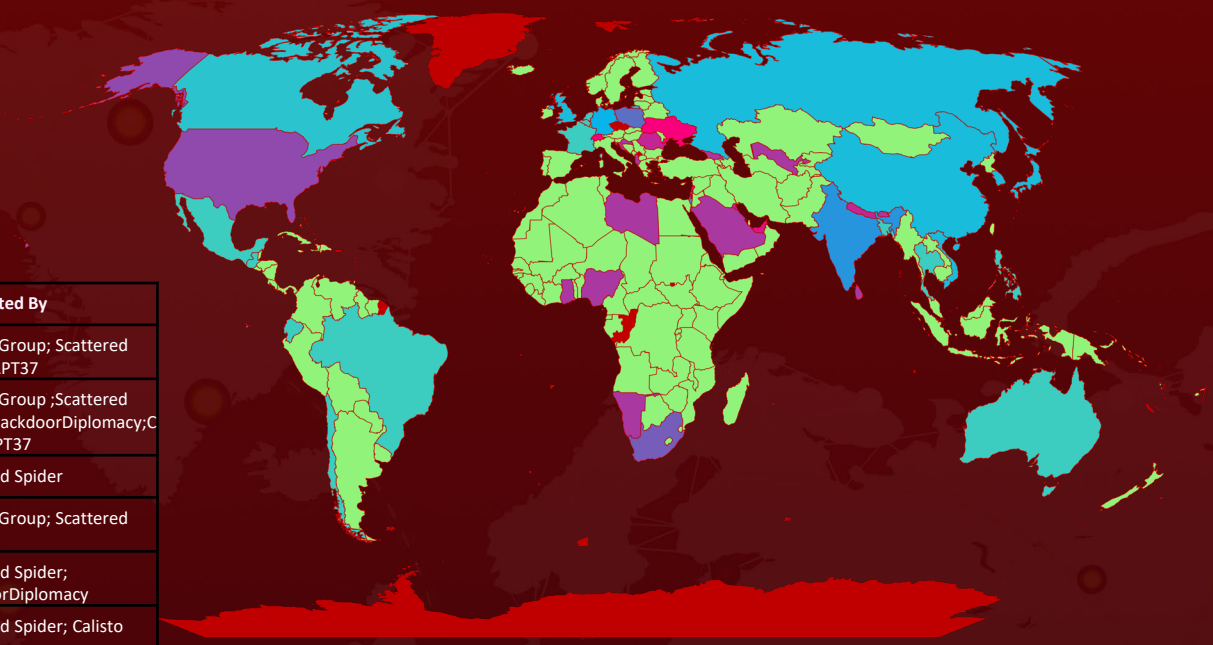
APT37 (unattributed)
North Korean hackers identified as APT37 exploited Internet Explorer zero-day (CVE-2022-41128) vulnerability to infect South Koreans and North Korean defectors and have employed a wide spectrum of malware, including backdoors such as Bluelight, Dolphin, and Rokrat, in their previous attacks.

Agrius (Fantasy Wiper)
Iran-based Agrius group has targeted Israel and the United Arab Emirates since 2020. The group deployed a wiper called Fantasy Wiper, disguised as ransomware, which was later modified into full-fledged ransomware.

*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Key Takeaways

Actor Map



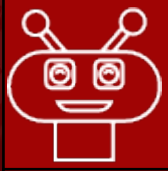
Color	Targeted By
	Lazarus Group; Scattered Spider;APT37
	Lazarus Group ;Scattered Spider;BackdoorDiplomacy;Calisto;APT37
	Scattered Spider
	Lazarus Group; Scattered Spider
	Scattered Spider; BackdoorDiplomacy
	Scattered Spider; Calisto

Actor Details

ICON	NAME	ORIGIN	MOTIVE
	Lazarus Group(Labyrinth Chollima,Group 77,Hastati Group,Whois Hacking Team,NewRomanic Cyber Army Team,Zinc,Hidden Cobra,Appleworm,APT-C-26,ATK 3,SectorA01,ITG03,TA404)	North Korea	Information theft and espionage, Sabotage and destruction, Financial crime
	Scattered Spider	Unknown	Financial crime
	BackdoorDiplomacy	China	Information theft and Espionage

*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Key Takeaways

ICON	NAME	ORIGIN	MOTIVE
	Calisto(Cold River, Nahr el bared, Nahr Elbard, Cobalt Edgewater, TA446, Seaborgium, TAG-53)	Russia	Information theft and Espionage
	APT 37 (Reaper,TEMP.Reaper,Ricochet Chollima,ScarCruft,Thallium,Group 123,Red Eyes,Geumseong121,Venus 121,Hermit,InkySquid,ATK 4,ITG10)	North Korea	Information theft and espionage
	Agrius(DEV-0227)	Iran	Information theft and espionage, Sabotage and destruction

*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Key Takeaways

Attacks

BlackHunt, NYX, Redeemer, Vohuk, and Amelia ransomware (unattributed)
These five ransomware families are attacking open RDP ports. The executable encrypts the victim's system and drops a ransom note named “Read Me.TXT”.

AppleJeus (Lazarus Group, DEV-0139)
It was initially discovered in 2018 and was primarily intended to collect information about the infected system and download shellcode from a C2 server. A notable feature in recent AppleJeus samples is that all strings and API calls are now obfuscated using a customized algorithm, making them less detectable by monitoring software.

Irafau, Quarian, ToRat, Asyncrat, and Merlin Backdoors (BackdoorDiplomacy)
Irafau, and Quanrain are custom tool backdoors, and ToRat, Asyncrat, and Merlin are open-source tool backdoors. All these backdoors are conducting reconnaissance, moving laterally around the victim's environment, and eluding detection.

BlackMagic (unattributed)
This latest BlackMagic ransomware targets its victims using a double extortion approach in which it initially exfiltrates the victim's data, followed by encryption, and has primarily targeted several firms in Israel's transportation and logistics niche.

ZeroBot (Unattributed)
‘Zerobot’ has two variants, both are written in Go programming language, the first variant discovered on 18 Nov 2022, and within a short time on 24 Nov 2022 second variant was developed and is more sophisticated and has several advanced features, which includes self-propagation, self-replication and attacks for different protocols.

Bluelight, Dolphin, and Rokrat (APT37)
These backdoors were used by group APT 37 in a recent Internet Explorer zero-day vulnerability to infect South Koreans, North Korean defectors, policymakers, journalists, and human rights activists.

*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Key Takeaways

Attacks

Fantasy Wiper (Agrius)

The Fantasy wiper is based on the previously mentioned Apostle wiper, however, unlike Apostle, Fantasy does not try to pass itself off as ransomware. Agrius APT hacking group used 'Fantasy' data wiper in supply-chain attacks impacting organizations in Israel, Hong Kong, and South Africa

TOP MITRE ATT&CK TTPS:

T1588 Obtain Capabilities	**T1588.006** Vulnerabilities	**T1059** Command and Scripting Interpreter	**T1190** Exploit Public-Facing Application	**T1082** System Information Discovery
T1574 Hijack Execution Flow	**T1204** User Execution	**T1489** Service Stop	**T1036** Masquerading	**T1566** Phishing
T1059.003 Windows Command Shell	**T1105** Ingress Tool Transfer	**T1210** Exploitation of Remote Services	**T1486** Data Encrypted for Impact	**T1548** AbuseElevation Control Mechanism
T1529 System Shutdown/Reboot	**T1070** Indicator Removal	**T1587** Develop Capabilities	**T1078** Valid Accounts	**T1499** Endpoint Denial of Service
T1027 Obfuscated Files or Information	**T1547** Boot or Logon Autostart Execution	**T1134** Access Token Manipulation	**T1055** Process Injection	**T1189** Drive-by Compromise

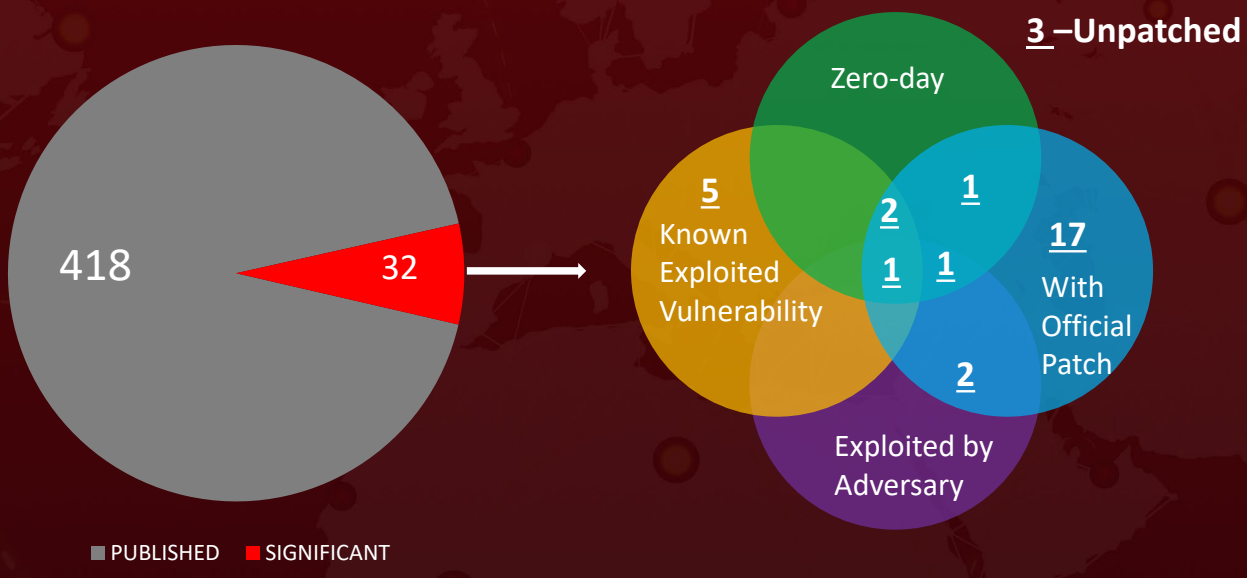
*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Key Takeaways

Vulnerabilities

Five Zero-Days & 27 Notable Mentions

Among the five zero-days, one was found in google chrome(CVE-2022-4262), BackdoorDiplomacy leveraged (CVE-2021-26855) to target telecom industry in Middle-east, CVE-2022-41128 an Internet Explorer exploited by APT37 and (CVE-2022-22965 & CVE-2017-17215) two leveraged by Zerobot. Multiple ransomware groups used CVE-2019-0708 to target open RDP ports. Scattered spider group leveraged CVE-2021-35464 to get access to mobile carriers' networks and perform SIM swapping.



*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **32 significant vulnerabilities** and block the indicators related to the threat actor **Lazarus Group**, **Scattered Spider**, **BackdoorDiplomacy**, **Calisto**, **APT37**, **Agrius** and malware **BlackHunt**, **NYX**, **Redeemer**, **Vohuk**, **Amelia ransomware**, **AppleJeus**, **Irafau**, **Quarian**, **ToRat**, **Asyncrat**, **Merlin Backdoors**, **BlackMagic**, **ZeroBot**, **Bluelight**, **Dolphin**, **Rokrat** , and **Fantasy Wiper**.

Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers and they can get comprehensive insights into their threat exposure and can action it effortlessly over the HivePro Uni5 dashboard by

- Running a Scan to discover the assets impacted by the **32 significant vulnerabilities**
- Testing the efficacy of their security controls by simulating the attacks related to and malware **BlackHunt**, **NYX**, **Redeemer**, **Vohuk**, **Amelia ransomware**, **AppleJeus**, **Irafau**, **Quarian**, **ToRat**, **Asyncrat**, **Merlin Backdoors**, **BlackMagic**, **ZeroBot**, **Bluelight**, **Dolphin**, **Rokrat** , and **Fantasy Wiper** in Breach and Attack Simulation(BAS)

Recommendations

Threat Advisories

Check out the links below for more extensive remediation and security precautions.

Multiple Ransomware groups targets open RDP Ports

Google Chrome's ninth zero-day in 2022

Recent Lazarus campaign leveraged Crypto App to spread AppleJeus malware

Attackers target Telecommunications sector to gain network access

Buffer Overflow vulnerability in FreeBSD

BackdoorDiplomacy targets the telecom industry in the Middle East

Linux flaws could be chained together to achieve root access

BlackMagic Ransomware disrupts the Israeli logistics sector

US Defense & NGOs fall prey to Russian hackers

New Botnet named Zerobot Exploiting Multiple Vulnerabilities

Fortinet addresses Authentication Bypass in addition to numerous flaws

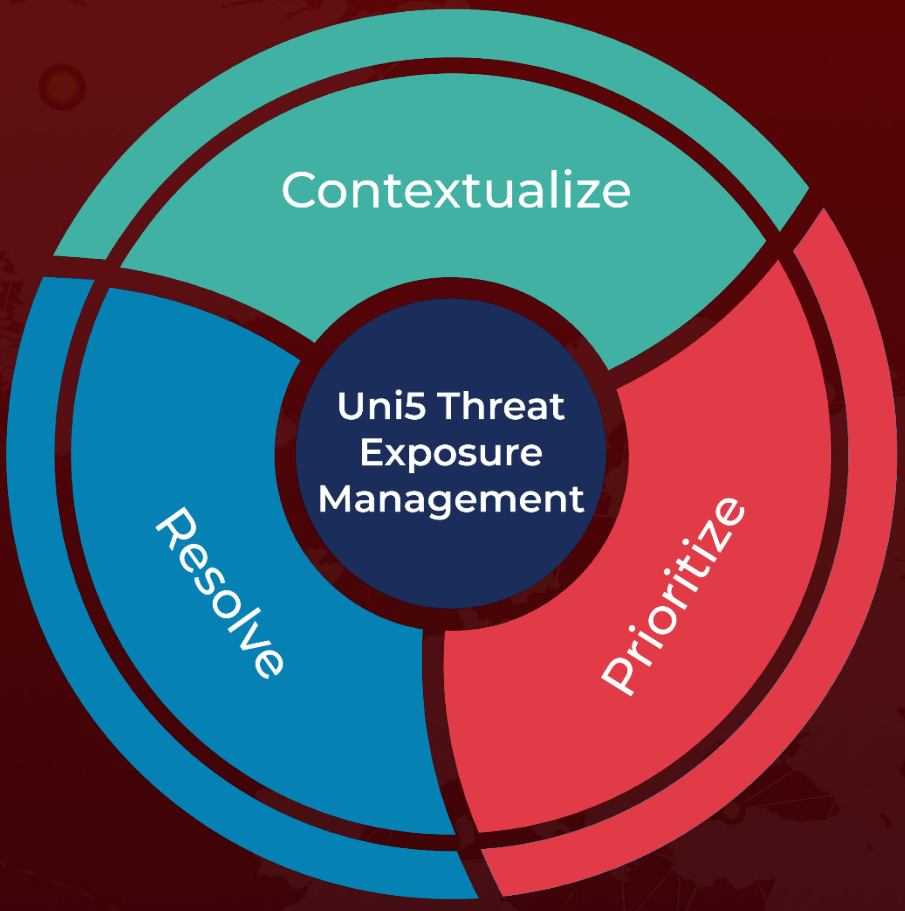
Internet Explorer Zero-Day Vulnerability Exploited by APT 37

Iran-based Agrius deploys Fantasy wiper to attack IT firms in Israel

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**:Threat Exposure Management Platform.



REPORT GENERATED ON

December 12, 2022 • 5:35 AM

More at www.hivepro.com